

that more people will be searched. Is routinely exposing images of our naked bodies to guards an acceptable trade-off of privacy for security?

The government is funding development of a variety of devices that can search through a person's clothing from a distance, without the person's knowledge or cooperation, to detect hidden weapons. These devices have valuable security applications, but the technology can be used for random searches, without search warrants or probable cause, on unsuspecting people. Clearly, guidelines are needed for acceptable uses of such machines.

WHO'S GOT YOUR PICTURE?

We are used to security cameras in banks and convenience stores. They deter crime and help in investigations of crimes. Prisons use video surveillance systems (sometimes called CCTV, for closed circuit television) for security; gambling casinos use them to watch for known cheaters. Video surveillance systems monitor traffic and catch traffic-law violators. Cameras alone raise some privacy issues. When combined with face-recognition systems, they raise even more. We describe some applications of face recognition and some relevant privacy and civil-liberties issues.

In 1999, a private company bought the digitized driver photos maintained by the motor-vehicle departments in several states. The company said it was buying the photos and building the database, which included other personal information such as Social Security numbers, to provide security services, for example to protect against credit fraud. Drivers had no choice about whether their photos were sold. Later it was disclosed that the U.S. Secret Service provided technical assistance and \$1.46 million in funding for the project. The Secret Service supported the project to fight terrorism, illegal immigration, and "identity crimes."* Publicity about the project generated public protest, and some states decided not to sell their driver photos.³³

The Tampa, Florida police used a computer system to scan the faces of all 100,000 fans and employees who entered the 2001 Super Bowl (causing some reporters to dub it Snooper Bowl). The system searched computer files of criminals for matches, giving results within seconds. People were not told they were being photographed. Later Tampa installed a similar system in a neighborhood of popular restaurants and nightclubs. Police in a control room zoom in on individual faces and check for matches in their database of suspects.³⁴ After September 11, 2001, several airports installed face-recognition systems, and police cameras in Washington, D. C. zoomed in on individuals a half mile away.

The ACLU has compared the use of the face-recognition system at the Super Bowl to a computerized police lineup, to which innocent people were subject without their knowledge or consent. Face-recognition systems had an accuracy rate of little more than 50% in the early 2000s. (Photos in databases tend to be old, and the systems do not perform well on images taken from different angles and in different lighting conditions.)

*The Secret Service has responsibility for investigating some kinds of financial and computer crime, in addition to its better-known role of protecting the President.

Harvard research fellow David Banisar argued that the low accuracy rate could result in the detention of many innocent people.³⁵ The accuracy will likely improve, but other issues will remain.

There are more than 500,000 CCTV cameras in England, many outdoors in public places to deter crime. A Londoner is likely to be recorded dozens of times a day. Government officials in a suburb of London said the CCTVs were responsible for 500 arrests in one year. Others argue that the cameras have not reduced crime. Defense lawyers complain that prosecutors sometimes destroy footage that might clear a suspect. A study by a British university found a number of abuses by operators of surveillance cameras, including collecting salacious footage, such as people having sex in a car, and showing it to colleagues.³⁶ A traffic monitoring system in Florida was removed after engineers were observed zooming in on individual pedestrians unrelated to traffic flow.

Is enforcing a 9 PM curfew for young people, one of the uses of public cameras in England, important enough to accept the potential abuses? Even if one thinks government curfews for young people are reasonable (and many do not), this application suggests the kind of monitoring and control of special populations made easy by the cameras. Banisar asks whether face-recognition systems would be used to track political dissidents, journalists, political opponents of powerful people—the kinds of people who were targeted for illegal or questionable surveillance in the past. More fundamentally, is this level of surveillance, with its potential for abuse, compatible with our notions of privacy and a free society? Not to 500 people who complained when the California Department of Transportation photographed their license plates and then contacted them for a survey on traffic in the area where they drove. These people objected vehemently to what they considered unacceptable surveillance by a government agency even when it was only their license plates, not their faces, being photographed for a survey, not a police action. Several city governments considered using cameras in public places, but decided not to. Toronto city officials refused to let police take over their traffic cameras to monitor a protest march and identify its organizers. In a controversial statement, the Privacy Commissioner of Canada argued that the country's Privacy Act required a "demonstrable need for each piece of personal information collected" to carry out government programs and therefore recording activities of large numbers of the general public was not a permissible means of crime prevention.³⁷

Many applications of CCTV and face-recognition systems are reasonable, positive uses of the technology for security and crime prevention. But there is a clear need for controls, guidelines, and some limitations. How should we distinguish appropriate from inappropriate uses? Should international events such as the Olympics, which are sometimes terrorist targets, use such a system? Should technologies like face-recognition systems be used only to catch terrorists and suspects in serious crimes, or should they be used in public places to screen for people with unpaid parking tickets? Should people be informed about when cameras are in use? If we consider these issues early enough, we can design some privacy-protecting features into the technology and consider appropriate privacy-protecting legislation before, as the Supreme Court of Canada worries in the quote that follows, "privacy is annihilated."